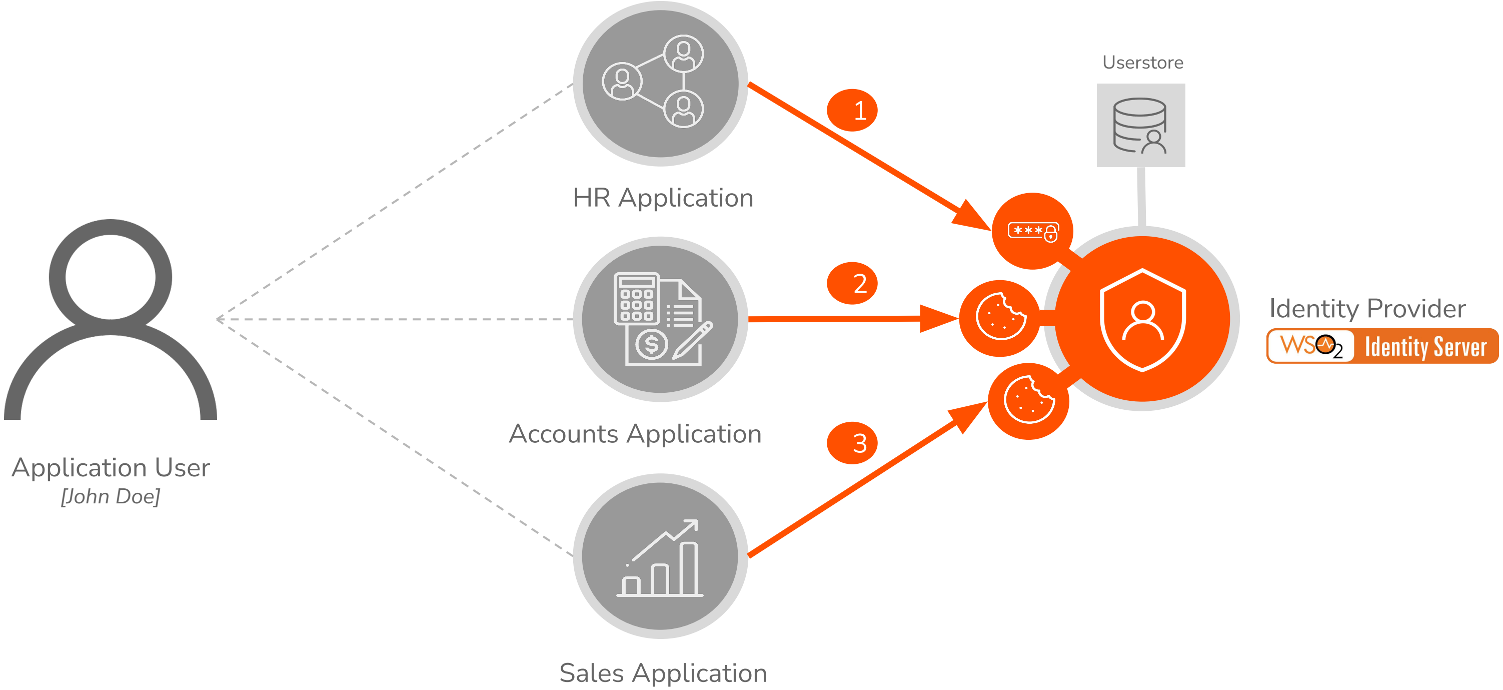
Single Sign-On with OpenID Connect

What is Single Sign-On

Sign in to one application and gain access to all the other applications sharing the same session



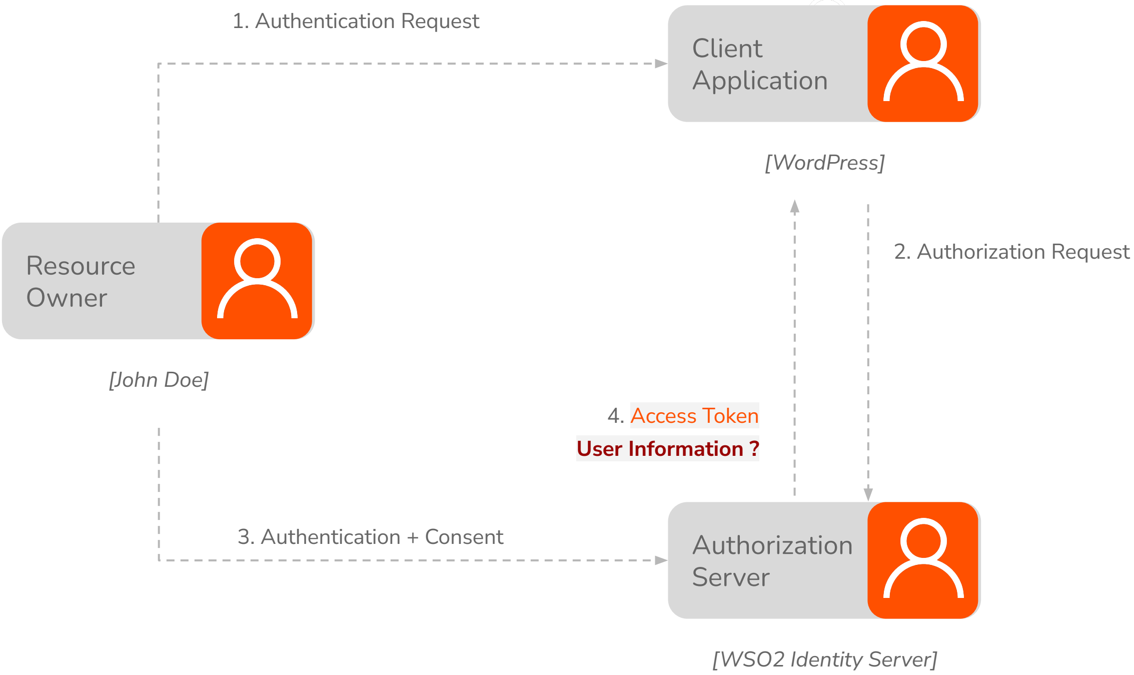
What is OpenID Connect (OIDC)

OpenID Connect 1.0 is a simple identity layer on top of the OAuth 2.0 protocol. It allows Clients to verify the identity of the End-User based on the authentication performed by an Authorization Server, as well as to obtain basic profile information about the End-User in an interoperable and REST-like manner.

Reference: https://openid.net/connect/

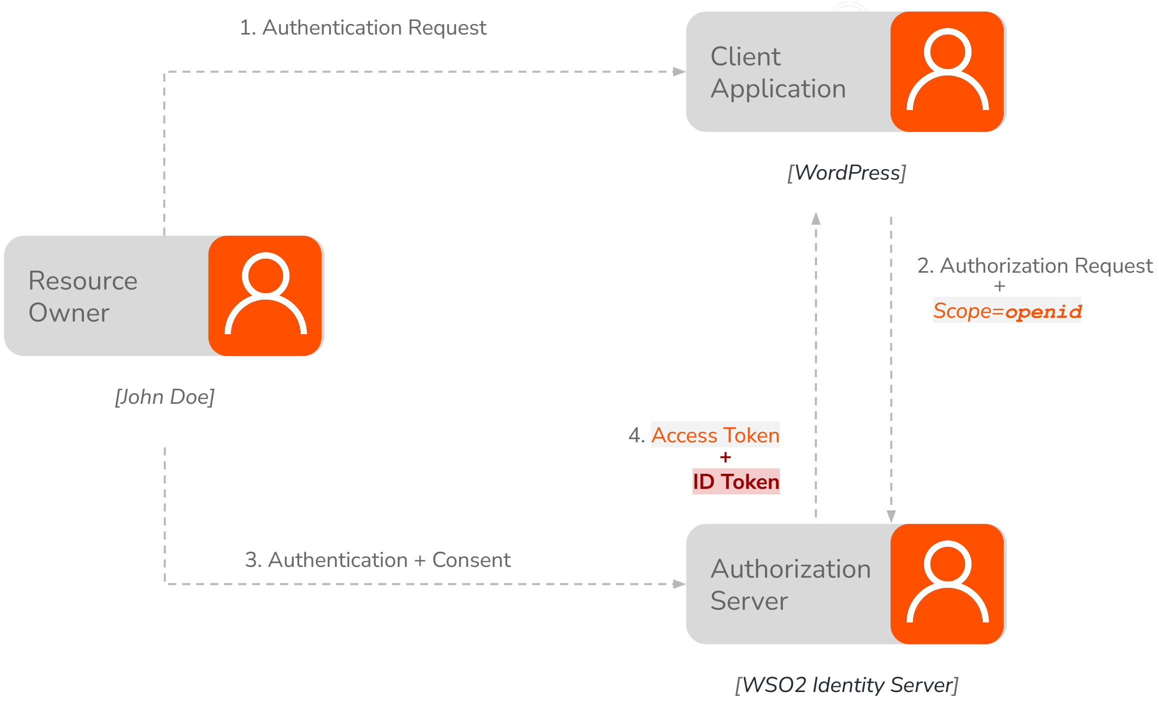
OAuth 2.0 Based Authentication

What’s missing in OAuth 2.0



OAuth 2.0 vs. OIDC

Authentication flow



1. Authentication Request

Client Application

[WordPress]

2. Authorization Request + Scope=**openid**

Resource Owner

[John Doe]

4. Access Token + **ID Token**

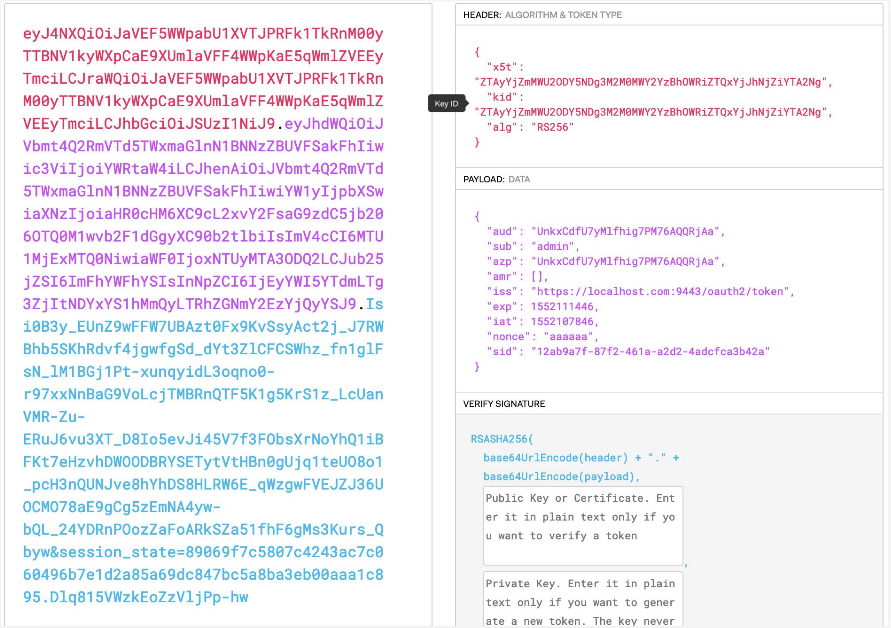
3. Authentication + Consent

Authorization Server

[WSO2 Identity Server]

ID Token Format

- Header
- Body/Payload
  - iss: issuer identifier
  - sub: subject identifier
  - aud: audience(s) that this ID Token is intended for
  - exp: the expiration time
  - iat: the token issued time
- Signature



```
eyJ4NXQiOiJaVEF5WWpabU1XVTJPRFk1TkRnM00y
TTBNV1kyWXpCaE9XUmlaVFF4WWpKaE5qWmlZVEEy
TmciLCJraWQiOiJaVEF5WWpabU1XVTJPRFk1TkRn
M00yTTBNV1kyWXpCaE9XUmlaVFF4WWpKaE5qWmlZ
VEEyTmciLCJhbGciOiJSUzI1NiJ9.eyJhdWQiOiJ
Vbmt4Q2RmVTd5TWxmaGlnN1BNNzZBUVFSakFhIiw
ic3ViIjoiYWRtaW4iLCJhenAiOiJVbmt4Q2RmVTd
5TWxmaGlnN1BNNzZBUVFSakFhIiwiYW1yIjpbXSw
iaXNzIjoiaHR0cHM6XC9cL2xvY2FsaG9zdC5jb20
6OTQ0M1wvb2F1dGgyXC90b2tlbiIsImV4cCI6MTU
1MjExMTQ0NiwiaWF0IjoxNTUyMTA3ODQ2LCJub25
jZSI6ImFhYWFhYSIsInNpZCI6IjEyYWI5YTdmLTg
3ZjItNDYxYS1hMmQyLTRhZGNmY2EzYjQyYSJ9.Is
i0B3y_EUnZ9wFFW7UBAzt0Fx9KvSsyAct2j_J7RW
Bhb5SKhRdvf4jgwfgSd_dYt3ZlCFCSWhz_fn1glF
sN_lM1BGj1Pt-xunqyidL3oqno0-
r97xxNnBaG9VoLcjTMBRnQTF5K1g5KrS1z_LcUan
VMR-Zu-
ERuJ6vu3XT_D8Io5evJi45V7f3FObsXrNoYhQ1iB
FKt7eHzvhDWOODBRYSETytVtHBn0gUjq1teUO8o1
_pcH3nQUNJve8hYhDS8HLRW6E_qWzgwFVEJZJ36U
OCMO78aE9gCg5zEmNA4yw-
bQL_24YDRnPOozZaFoARkSZa51fhF6gMs3Kurs_Q
byw&session_state=89069f7c5807c4243ac7c0
60496b7e1d2a85a69dc847bc5a8ba3eb00aaa1c8
95.Dlq815VWzkEoZzVljPp-hw
```

HEADER: ALGORITHM & TOKEN TYPE

```
{
  "x5t":
"ZTAyYjZmMWU2ODY5NDg3M2M0MWY2YzBhOWRiZTQxYjJhNjZiYTA2Ng",
  "kid":
"ZTAyYjZmMWU2ODY5NDg3M2M0MWY2YzBhOWRiZTQxYjJhNjZiYTA2Ng",
  "alg": "RS256"
}
```

PAYLOAD: DATA

```
{
  "aud": "UnkxCdfU7yMlfhig7PM76AQQRjAa",
  "sub": "admin",
  "azp": "UnkxCdfU7yMlfhig7PM76AQQRjAa",
  "amr": [],
  "iss": "https://localhost.com:9443/oauth2/token",
  "exp": 1552111446,
  "iat": 1552107846,
  "nonce": "aaaaaa",
  "sid": "12ab9a7f-87f2-461a-a2d2-4adcfca3b42a"
}
```

VERIFY SIGNATURE

```
RSASHA256(
  base64UrlEncode(header) + "." +
  base64UrlEncode(payload),
  Public Key or Certificate. Ent
  er it in plain text only if yo
  u want to verify a token
  ,
  Private Key. Enter it in plain
  text only if you want to gener
  ate a new token. The key never
```

Identity Layer

- **Who** is the user got authenticated
- **Where** was the user authenticated
- **When** was the user authenticated
- **How** was the user authenticated
- **What** attributes the user can give you

Authorization Flows

- Authorization Code
- Implicit
- Hybrid

OIDC Specifications

- Core – Defines the core OpenID Connect functionality
- Discovery – Defines how Clients dynamically discover information about OpenID Providers
- Dynamic Registration – Defines how clients dynamically register with OpenID Providers
- Session Management – Defines how to manage OpenID Connect sessions
- Front-Channel Logout – Defines a front-channel logout mechanism
- Back-Channel Logout – Defines a logout mechanism that uses direct back-channel communication between the OP and RPs being logged out

Quick Recap

What you learnt

1. About Single Sign-On (SSO)
2. What’s missing in OAuth2
3. ID token and identity layer
4. Authorization flows

Any Questions ?

Reach us through the following channels

✉ iam-dev@wso2.org

https://stackoverflow.com/questions/tagged/wso2-identity-server

https://discord.com/invite/Xa5VubmThw

Thanks!

wso2.com